UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,502	12/31/2003	Soo-Hyung Lee	51876P585	1208

8791 7590 06/16/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
NOORISTANY, SULAIMAN	

ART UNIT	PAPER NUMBER
2446	

MAIL DATE	DELIVERY MODE
06/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,502	LEE ET AL.	
	Examiner	Art Unit	
	SULAIMAN NOORISTANY	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/31/2003, 11/25/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

This Office Action is response to the application (10749502) filed on 04/16/2009.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114. including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 7 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/18/08 has been entered.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-2, 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Liang** U.S. Patent Application Publication No **US 20040205419** in view of **Porras** U.S. Patent Application Publication No. **US 2003/0212903** further in view of **Gupta** U.S. Patent No. **US 7,234,168** further in view of **Ishikawa** U.S Patent app. No. **US 2007/0079367** further in view of **Brendel** U.S. Patent Application Publication No. **US 20050125195**.

Regarding claim 1, Liang teaches wherein a method for detecting abnormal traffic at the network level using a statistical analysis, the method comprising the steps of:

a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data for approximating an overall network traffic level **(FIG. 4, the data collected in the client devices 112, 120 and 124 are transferred to the server 108 through uplink data paths 1121, 1201 and 1241, respectively. The data from the client devices 112, 120 and 124 are then processed in the correlative rules engine (CRE) 106. The correlative rules engine 106 analyzes data from all of the client devices, which also includes the ability to maintain and keep track of a plurality of alert levels occurring in different sensors with different client devices – [0043]).**

With respect to claim 1, Liang teaches the invention set forth above except for the claimed "*extracting a characteristic network traffic data corresponding to the overall network traffic level*".

Porras further teaches wherein a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data in the network level **(Fig. 1, unit 12a –12c indicating the integrated of different domains in a network)**;

b) extracting a characteristic network traffic data based on the traffic data in the network traffic level (**characteristic data forms from the header of the packet [0032]**);

c) comparing the characteristic network traffic data with a predetermined

characteristic traffic data profile resulting from statistical computations and representing normal traffic (**Fig. 5, unit 78 (compare one of the short-term profiles to a corresponding long-term statistical profile)**, and determining whether there is abnormal traffic at the network level (**Fig. 4, unit 70 (Determine if statistical profile is abnormal**);

d) updating the predetermined characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, and analyzing volume amount of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic at the network level (**the monitor can respond by reporting (updating) the activity (i.e. seriousness of the abnormal traffic like privilege network errors and abnormal levels of the network level) to another monitor or by executing a countermeasure response [0071]**).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Liang's invention by utilizing a method of network surveillance includes receiving network packets handled by a network entity and building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. A comparison of the statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity, as taught by Porras.

However, Porras teaches the invention set forth above except for the claimed "*a single traffic sensing module*".

Gupta teaches that is well known to have traffic a single sensing module **(Fig. 2, unit 52 – Sensor Management Module** "A single sensor management system may be used to control multiple sets of primary sensors and redundant sensors"**).**

e) transmitting the analysis result of the volume amount of the abnormal traffic to an abnormal traffic processing system **(the overall volume of discarded packets as well as a measure analyzing the disposition of the discarded packets (abnormal packet) can provide insight into unintentionally malformed packets resulting from poor line quality or internal errors in neighboring hosts [0076]).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Liang's invention by utilizing a network security sensors and distributed network security sensor architectures used to implement intrusion detection and protection. In addition, a sensor management system is associated with a sensor or set of sensors. The sensor management system provides supervisory control of a sensor. The sensor management system may be used to implement a shared-resource virtual intrusion detection system, as discussed below. A single sensor management system may be used to control multiple sets of primary sensors and redundant sensors. The combination of the sensor, redundant sensor, and sensor management system is referred to as a local sensor security module. Furthermore, as it's disclosed the local sensor security modules may be distributed throughout a network. In this example, local sensor security modules 27_1 through 27_N are positioned between an enterprise network and Internet service providers 28_1 through

28_N. In addition, a local sensor security module 27_0 is positioned between the enterprise network and a protected server, as taught by Gupta.

However, Gupta is silent in terms of *"to detect abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure."*

Ishikawa teaches wherein to detect abnormal traffic without operation of a network manager **(abnormal traffic patterns – [0041])**, and processing the abnormal traffic to prevent a network failure **(the traffic analyzer 30 instructs the switching device 18 to cease announcing the server network address to the offending network – [0041]).**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Liang's invention by utilizing the attempts to eliminate fraudulent requests to a server, or its firewall, are limited to blocking the source address, and preventing repeated requests to respond to one address via blocking the request. Although these mechanisms can prevent fraudulent requests from being sent to, or received by, the server, to prevent the transmission of requests from the suspected traffic, the network device receiving the requests, such as, the routers or firewall, must review each incoming packet. Thus, although these requests can be identified, the identification of these requests require that the network device, such as, the router or firewall, look at each incoming packet to determine whether to block the transmission. As such, these solutions do not prevent the stifling of traffic flow and often still result in the router, firewall or server from being paralyzed as the problem is merely shifted between the devices within the network. ***Furthermore, detection system utilizes an***

activity monitoring system which monitors network devices, such as routers and firewalls, and determines whether abnormal activity or traffic patterns are emerging on the devices. If a determination is made that abnormal activity or abnormal traffic patterns exist, the activity monitoring system responds by blocking the activity or redirecting the traffic, as taught by Ishikawa.

Brendel further teaches wherein to detect abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure **(provides a traffic evaluation device including a data interface to receive one or both of network traffic and data indicative of characteristics of network traffic and including processing means operable to evaluate the network traffic and/or data received by said data interface for predetermined characteristics that indicate that the network traffic contains a subset of attack traffic, and upon detection of said predetermined characteristics retrieve from memory information defining a superset and provide an output defining said superset – [0023]);**

Brendel further teaches wherein gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data for approximating an overall network traffic level **(By having multiple observation points, overall traffic ratios and statistics within the subnet or section of the network may be monitored – [0126])** in order to make the system more efficient and defines the network traffic level.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Liang's invention by utilizing modules that each evaluate data received and may implement filters to redirect or block particular packets dependent on the result of the evaluation and according to predetermined criteria. Those skilled in the relevant arts will appreciate that many different filtering strategies exist and more are continually being developed. An advantage of the present invention is that it is anticipated that future traffic evaluation/filtering/management modules may be relatively easily added to the apparatus, as taught by Brendel.

Regarding claim 2, Liang, Porras, Gupta, Ishikawa and Brendel together taught the method as in claim 1 above. Porras further teaches wherein the characteristic traffic data includes:

information on traffic assigned to an application port which is selected according to an application service (**TCP port identifier [0036]**);

information on traffic of which packet size is identical (**network measures number of packets and number of kilobytes [0037]**); and

information on traffic of which the number of source-destination pairs, which represents the number of source addresses of the traffic having the same target address (**categorical measures including the network source and destination address [0036], packet source addresses and destination addresses match is given internal host [0033]**).

Claim 4 list all the same elements of **claim 1**, but in computer readable medium rather than method form. Therefore, the supporting rationale of the rejection to **claim 1** applies equally as well to **claim 4**.

Response to Arguments

Applicant's arguments with respect to claim1-2, 4 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can normally be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu, can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sulaiman Nooristany 06/10/2009

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446